准备迁移

适用于防火墙迁移工具的准则和限制

Fortinet 配置

您的 Fortinet 配置必须满足以下要求：

- Fortinet 配置支持迁移，如 支持的迁移平台，第 6 页 中所述。
- Fortinet 版本支持迁移，如 支持迁移的软件版本，第 7 页 中所述。

（可选）目标 威胁防御 设备

当您迁移到 Cisco Secure Firewall Management Center 时，它可能已添加目标 威胁防御 设备，也可能未添加。

您可以将共享策略迁移到 管理中心，以便将来部署到 威胁防御 设备。要将设备特定的策略迁移到威胁防御，必须将其添加到 管理中心。

- 您的目标 威胁防御 设备必须满足以下要求：
  - 设备满足硬件设备的准则，如此中所述： 适用于 威胁防御设备的准则和限制，第 6 页
  - 设备支持作为迁移的目标，如支持的迁移平台，第 6 页中所述。
  - 威胁防御 软件版本支持迁移，如支持迁移的软件版本，第 7 页中所述。
  - 威胁防御 设备已在 管理中心 上注册。

管理中心

- 管理中心软件版本支持迁移，如支持迁移的软件版本，第 7 页中所述。
- 您已获取并安装 威胁防御 的智能许可证，包括您计划从 Fortinet 接口迁移的所有功能，如下所述：
- Cisco.com 上的思科智能账户“入门指南”部分。
- 在思科智能软件管理器中注册防火墙管理中心。
- 许可防火墙系统
- 防火墙迁移工具 3.0 现在支持迁移到云交付的防火墙管理中心，如云交付的防火墙管理中心迁移中所述。

防火墙迁移工具

- 确保您用来运行防火墙迁移工具的计算机符合相关要求，如防火墙迁移工具的平台要求，第 8 页中所述。
- 防火墙迁移工具允许您在以下限制内配置批量推送的批处理大小：

配置项目	批处理大小限制	默认值
对象	500	50
ACL	1000	1000
NAT	1000	1000
路由	1000	1000

注释 对于对象，API 批处理大小不能超过 500。防火墙迁移工具将值重置为 50 并继续批量推送。

对于 ACL、路由和 NAT 规则，每个批处理大小不能超过 1000。防火墙迁移工具将值重置为 1000 并继续批量推送。

您可以在 `app_config` 文件中配置批处理大小限制，该文件位于：*`<migration_tool_folder>`*`\app_config.txt`.

注释 重启应用以使更改生效。

- 开始从防火墙迁移工具推送配置之后，不要在管理中心中对配置进行任何更改或更新，直至迁移完成。

适用于 Fortinet 防火墙配置的准则和限制

在转换期间，防火墙迁移工具会为所有支持的对象和规则创建一对一映射，而无论它们是否用于规则或策略。防火墙迁移工具提供优化功能，允许您在迁移中排除未使用的对象（任何 ACL 和 NAT 中未引用的对象）。

防火墙迁移工具处理如下不受支持的对象和规则：

- 不受支持的接口、对象、NAT 规则和路由不会被迁移。
- 不受支持的 ACL 规则将作为禁用的规则迁移到管理中心。

Fortinet 防火墙配置文件

您可以手动获取 Fortinet 防火墙配置文件。

您手动导入到防火墙迁移工具中的 Fortinet 防火墙配置文件必须满足以下要求：

- 具有从 Fortinet 设备导出的运行配置。防火墙迁移工具支持从全局和每 VDOM 导出进行配置备份。有关详细信息，请参阅导出 Fortinet 配置文件。
- 仅包含有效的 Fortinet 防火墙配置。
- 不包含语法错误。
- 具有扩展名为 .conf 或 .txt 的文件类型。
- 使用 UTF-8 文件编码。
- 尚未手工编码或手动更改。如果您修改了 Fortinet 防火墙配置，则建议您在 Fortinet 防火墙设备上测试修改后的配置文件，以确保它是有效的配置。

Fortinet 防火墙配置限制

源 Fortinet 防火墙配置的迁移存在以下限制：

- 系统配置未迁移。
- 防火墙迁移工具不支持迁移被应用于 50 个或更多接口的单个 ACL 策略。您必须手动迁移已应用于超过 50 个或更多接口的 ACL 策略。
- 您无法将 Fortinet 防火墙配置（例如动态路由和 VPN）迁移到威胁防御。手动迁移这些配置。
- 不支持类型为虚拟线路、冗余接口、隧道接口、vdom-link 和 SDwan 接口或区域的 Fortinet 防火墙接口，它们不会被迁移。

  Fortinet 硬件或软件交换机逻辑接口将作为 FTD L3 接口进行迁移。硬件或软件交换机成员接口不会使用防火墙迁移工具来进行迁移。
- 不支持迁移通配符 FQDN、通配符 IP、动态对象和排除组等对象。
- 无法迁移处于透明模式或透明 VDOM 的 Fortinet 防火墙设备。

- 管理中心不支持嵌套服务对象组和端口组。在转换过程中，防火墙迁移工具会扩展引用的嵌套对象组或端口组的内容。
- 防火墙迁移工具将一行中有源端口和目标端口的扩展服务对象或组拆分为跨多行的不同对象。对此类访问控制规则的引用将转换为具有完全相同含义的管理中心规则。

Fortinet 防火墙迁移指南

防火墙迁移工具会对威胁防御配置使用最佳实践。

ACL 日志迁移选项遵循对应于威胁防御的最佳实践。根据源 Fortinet 防火墙配置启用或禁用规则的日志选项。对于使用 **deny** 操作的规则，防火墙迁移工具会在连接开始时配置日志记录。如果操作是 **permit**，则防火墙迁移工具会在连接结束时配置日志记录。

支持的 Fortinet 防火墙配置

防火墙迁移工具可完整迁移以下 Fortinet 防火墙配置：

- 网络对象和组（通配符 FQDN、通配符掩码、Fortinet 动态对象除外）
- 服务对象
- 服务对象组（嵌套服务对象组除外）

注释 由于管理中心不支持嵌套，因此防火墙迁移工具会扩展引用规则的内容。但是，系统会迁移规则及完整功能。

- IPv4 和 IPv6 FQDN 对象与组
- IPv6 转换支持（接口、静态路由、对象、ACL 和 NAT）
- 访问规则
- NAT 规则
- 未迁移的静态路由、ECMP 路由
- 物理接口
- 子接口（子接口 ID 在迁移时会始终被设为与 VLAN ID 相同的编号）
- 汇聚接口（端口通道）
- 防火墙迁移工具支持将各个 VDOM 作为单独的威胁防御设备从 Fortinet 防火墙进行迁移。
- 基于时间的对象 - 当防火墙迁移工具检测到通过访问规则引用的基于时间的对象时，防火墙迁移工具会迁移基于时间的对象并映射这些对象与相应的访问规则。根据**优化、检查和验证配置**页面中的规则验证对象。

  基于时间的对象属于允许基于时间段进行网络访问的访问列表类型。如果您必须根据一天中的特定时间或一周中的特定天数限制出站或入站流量，则此类对象非常有用。

注释
- 您必须将时区配置从源 Fortinet 手动迁移到目标 FTD。
- 非 FTD 流不支持基于时间的对象，它们将被禁用。
- 防火墙管理中心版本 6.6 及更高版本支持基于时间的对象。

部分支持的 Fortinet 防火墙配置

防火墙迁移工具部分支持以下Fortinet防火墙配置的迁移。其中一些配置包括含高级选项的规则，这些规则在迁移后失去这些选项。如果管理中心支持这些高级选项，您可以在迁移完成后手动配置它们。

- 包含不受支持的地址对象的地址组。
- 所含服务对象的协议中包含 TCP 或 UDP 和 SCTP 的服务组。

注释 SCTP 协议将被删除，服务组将部分迁移。

不支持的 Fortinet 防火墙配置

防火墙迁移工具不支持以下Fortinet防火墙配置的迁移。如果这些配置在管理中心中受支持，您可以在迁移完成之后手动配置它们。

- 基于用户、基于设备和基于互联网服务 ID 的访问控制策略规则
- 带有不受支持 ICMP 类型和代码的服务对象
- 基于隧道协议的访问控制策略规则
- 配置有块分配选项的 NAT 规则
- 配置有 SCTP 的 NAT 规则
- 配置有主机“0.0.0.0”的 NAT 规则
- 源或目标中包含 FQDN 对象的 NAT 规则
- 以特殊字符开头或包含特殊字符的 FQDN 对象
- 通配符 FQDN
- Fortinet 允许配置结合了 IPv4 和 IPv6 的策略（合并策略）。

注释 防火墙迁移工具不支持此策略。

适用于 威胁防御设备的准则和限制

当您计划将 配置迁移到 威胁防御 时，请考虑以下准则和限制：

- 如果 威胁防御 上有任何现有的设备特定配置（例如路由、接口等），则在推送迁移期间，防火墙迁移工具会自动清除设备并从 配置执行覆盖。

注释 为防止设备（目标 威胁防御）配置数据意外丢失，我们建议您在迁移之前手动清理设备。

  Fortinet 硬件或软件交换机逻辑接口将作为 威胁防御 L3 接口进行迁移。硬件或软件交换机成员接口不会使用防火墙迁移工具来进行迁移。

  在迁移期间，防火墙迁移工具会重置接口配置。如果在策略中使用这些接口，则防火墙迁移工具无法重置它们，因此迁移会失败。

- 威胁防御 设备可以是独立设备或容器实例。它不能是集群或高可用性配置的一部分。
  - 如果目标 威胁防御 设备是容器实例，则必须至少具有与 相同数量的已使用物理接口、物理子接口、端口通道接口和端口通道子接口（不包括“管理专用”接口）；否则，必须在目标 威胁防御 设备上添加所需类型的接口。
    - 防火墙迁移工具不创建子接口，仅允许接口映射。
    - 它允许不同接口类型之间的映射，例如：物理接口可以映射到端口通道接口。

支持的迁移平台

以下 Fortinet 和 威胁防御 平台支持使用 防火墙迁移工具 进行迁移。有关支持的 威胁防御平台的更多信息，请参阅 Cisco Secure Firewall 兼容性指南 。

支持的目标 威胁防御平台

您可以使用 防火墙迁移工具将源 配置迁移到 威胁防御 平台的以下独立实例或容器实例：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Firepower 9300 系列包括：
  - SM-24

- SM-36
- SM-40
- SM-44
- SM-48
- SM-56

- VMware 上的威胁防御，使用 VMware ESXi、VMware vSphere Web 客户端或 vSphere 独立客户端部署

对于 Microsoft Azure 云，防火墙迁移工具支持迁移到 threat defense virtual。

有关 Azure 中 threat defense virtual 的前提条件和预先配置，请参阅 Cisco Secure Firewall Threat Defense Virtual 和 Azure 入门。

对于 AWS 云，防火墙迁移工具支持迁移到 threat defense virtual。

有关 AWS 云中 threat defense virtual 的必备条件和预先配置，请参阅 Threat Defense Virtual 前提条件。

对于每一个这些环境，防火墙迁移工具在按照要求进行预先配置后，都需要网络连接才能连接到 Microsoft Azure 或 AWS 云中的 管理中心，然后再将配置迁移到云中的 管理中心。

注释 要成功迁移，必须在使用 防火墙迁移工具之前完成 管理中心 或威胁防御虚拟的预先配置前提条件。

支持迁移的软件版本

以下是支持迁移的 Fortinet 和 威胁防御 版本：

支持的 Fortinet 防火墙版本

防火墙迁移工具支持迁移到运行 Fortinet 防火墙操作系统版本 5.0 及更高版本的 威胁防御。

源 Fortinet 防火墙配置支持的 管理中心 版本

对于 Fortinet 防火墙，防火墙迁移工具 支持迁移到运行 6.2.3.3 或更高版本的 管理中心 所管理的 威胁防御 设备。

注释 当前不支持迁移到 6.7 威胁防御 设备。因此，如果设备配置了用于 管理中心 访问的数据接口，则迁移可能会失败。

支持的 威胁防御版本

防火墙迁移工具迁移工具建议迁移到正在运行 威胁防御 版本 6.5 及更高版本的设备。

有关思科防火墙软件和硬件兼容性的详细信息（包括 威胁防御的操作系统和托管环境要求），请参阅思科防火墙兼容性指南。

防火墙迁移工具的平台要求

防火墙迁移工具对基础设施和平台的要求如下：

- 运行 Windows 10 64 位操作系统或者 macOS 10.13 或更高版本
- 使用 Google Chrome 作为系统默认浏览器
- (Windows)“电源和睡眠”中的“睡眠”设置配置为“从不让 PC 进入睡眠”，以便在大型迁移推送时系统不会进入睡眠状态
- (macOS) 配置了“节能模式”设置，以便在大型迁移推送时计算机和硬盘不会进入睡眠状态

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。